Punainen Risti

Data protection documentation
Created: 25 April 2018
Updated: 1 April 2025

FRC BRANCH DATA PROTECTION GUIDELINES

How to Handle Personal Data Safely and Legally in Branch Operations

Data Protection and the Finnish Red Cross

The data protection policy of the Finnish Red Cross (FRC) defines the principles and responsibilities of data protection within the FRC. The policy, approved by the Board, applies to all personal data processing carried out within the FRC or on its behalf, regardless of the origin, content, purpose or location of the data processing. The policy is accompanied by a tripartite agreement between the Central Office, districts and branches, which defines the roles and responsibilities of each party. The data protection policy and tripartite agreement can be found on the Volunteer Information data protection page: https://volunteerinfo.redcross.fi/data-protection.

Data Protection Principles

In general, FRC branches act as the data processors for the organisation and are responsible for ensuring that processing complies with the data protection policy, statements and guidelines. Privacy statements for personal data processing can be found on the organisation's data protection page: https://www.redcross.fi/data-protection/ .

The branch is responsible for ensuring that:

- Only necessary personal data is collected
- Individuals are informed of the purpose of data collection
- Personal data is used only for the purposes defined in the privacy statements
- Only authorised personnel have access to personal data
- Personal data is handled carefully and confidentially
- Outdated or unnecessary data is not retained
- Personal data is not disclosed outside the organisation without proper authorisation
- Email communication respects the recipient's privacy

Refer to the following materials:

- Volunteer Information data protection page: https://volunteerinfo.redcross.fi/data-protection
- FRC data protection policy and tripartite agreement
- FRC data protection contacts and their details

- FRC data protection page and privacy statements on https://www.redcross.fi/data-protection/

The FRC privacy statements are nationwide and apply to all processing of these personal data, regardless of where or by whom the data is physically processed. For example, the statements for volunteers and members describe the processing of their personal data throughout the organisation. FRC branches are also committed to processing data in accordance with these statements, so it is important to familiarise yourself with them. If you need more information, contact your district's data protection contact person.

Collecting, Using, and Disposing of Personal Data

1. Personal data may only be collected for a specific, predefined purpose. Collect only the data necessary for processing, not any extra or 'just in case' data.
2. Every form (electronic or paper) that collects personal data must include a statement of the intended use of the data, i.e. a link to the privacy statement or a paper copy of the statement.
3. Request marketing consent on forms. This allows for broader FRC communication in the future.
4. If a person has a secret address, or secret phone number, ensure they understand how their data will be processed.
5. Ensure personal data is stored securely and that only those with a legitimate need can access it.
6. Do not disclose personal data to third parties without permission.
7. If sending personal data via email, protect the file containing personal data with a password. Do not send the file and password in the same message. Preferably send the file via email and the password via text message. If texting is not possible, send the password in a separate email from the file.
8. Personal data must not be retained longer than necessary. Review systems, paper files and Excel sheets annually and dispose of unnecessary data.
9. When disposing of personal data, do so carefully and securely.

Processing of Personal Data in Cooperation with Authorities

In joint operations with the authorities, always follow the personal data handling instructions of the authority in question. The leading authority of the operation defines what data is collected and how. After the operation, all collected data is handed over to the authority. If any data is not handed over, it must be disposed of. Operations with the authorities cannot be publicly disclosed without permission and guidance, and recipients of aid must not be photographed.

Electronic Communications and Marketing

1) Information about branch activities and communications related to membership and volunteering may be sent to members and volunteers unless specifically prohibited.

2) A responsible volunteer cannot prohibit communication related to their volunteer task.
3) Marketing communication may not be sent without marketing consent. The marketing consent must be recorded in the OMA register.
4) When sending mass emails, ensure that recipients' email addresses are in the Bcc field, hidden from other recipients. A good practice is to mention in the message who the recipients are, e.g. “This message is sent to all the members/volunteers of branch x”.

Secure Data Practices

Data security is an essential part of protecting personal data. Much of data security depends on individual actions.

In practice, remember the following:

- Keep personal data out of sight and reach of outsiders.
- Do not discuss confidential matters in public places.
- Use a security code on mobile devices and a privacy screen on laptops.
- Lock your laptop when leaving it alone (Windows + L).
- Do not leave your laptop or phone in your car.
- Use passwords for WLANs, avoid open wireless networks – your mobile hotspot is safer.
- Use strong passwords and multi-factor authentication.
- Choose applications carefully and keep them updated.
- Restart your mobile device weekly.
- Be suspicious of strange emails and phone calls.

Information Systems

Whenever possible, store and process personal data in centralised systems like OMA, HUPSIS, and OHTO. Avoid separate Excel or paper lists except for temporary use.

If using or acquiring other systems like Google Docs or similar cloud services, remember:

- Use reputable service providers.
- Enable multi-factor authentication.
- Manage access rights with care.
- Regularly review and clean up accounts.
- Remove inactive users.
- Follow the principle of least privilege – access only as needed and for the necessary duration.

Personal Data Breaches

A personal data breach is an event where personal data is destroyed, lost, altered, disclosed without authorisation, or accessed by unauthorised parties.

Examples include:

- Lost data transfer device (e.g. USB stick)
- Stolen/lost computer or smartphone
- Sending documents with personal data to the wrong person
- Unauthorised use of an open computer/phone
- Mass email with all the addresses in the "To" field (if recipients are unknown to each other)
- Unauthorised viewing of personal data in a system
- Hacking, data breach
- Malware infection

Reporting Data Breaches

Report breaches as soon as possible. Even if caused by accident or carelessness, it's important to be aware of issues to minimise impact. Reporting is the right thing to do!

Report to:

- District data protection contact
- FRC data protection officer: tietosuoja@redcross.fi
- Within your branch: data protection contact and department chairman

Include the following in your report:

- What happened
- When and how the breach was discovered
- When the breach occurred
- Whose personal data was affected (e.g. members, volunteers)
- What personal data was affected (e.g. name, address, health data, membership info)
- How many individuals were affected

Reporting to Authorities and Data Subjects:

The district data protection contact and the FRC data protection officer assess the severity of the breach. Based on the assessment, they will make the required notifications to the authorities and affected individuals. The branch will be informed of the actions taken.

Rights of the Data Subject

Data subjects have broad rights regarding their data. Key rights include:

- Request deletion of their data

- Restrict processing of their data (e.g. remain a member but prohibit email communication)
- Access a copy of all data registered about them

Requests must be honoured unless there is a legal reason not to. For requests related to FRC systems, notify tietosuoja@redcross.fi.

Different FRC Registers and Their Use

Below are examples of lawful use of different personal data groups:

- Volunteer Data – Includes those who:
    - Have signed up as volunteers
    - Participated in activities
    - Attended volunteer training

  They may receive information about volunteer activities. Without marketing consent, they may not be invited to events like first aid courses unless it's part of their volunteer role.

- Member Data – Always use the latest list from OSSI or the region. Do not keep old lists. Members may receive information about department activities and invitations to events. If a member has prohibited email communication, it must be respected.
- Event Registrations – Data may only be used for the specific event unless marketing consent was requested during registration.
- Children's Personal Data – Handle minors' data with special care. For example, club and camp participants' data may only be used in connection with those activities. Do not market to minors. Digital services may not be offered to children under 13 without guardian consent.

Questions and Unclear Situations

Your primary contact is your branch's data protection contact. Support is also available from your district's data protection contact and the FRC data protection officer: tietosuoja@redcross.fi